Machine Translated by Google

International arbejdsgruppe om
databeskyttelse inden for teknologi

Arbejdspapir om centralbankers digitale valuta - CBDC

Udgivet 13 th Juni 2024 [1]

Indholdsfortegnelse

Resumé 2

1. Introduktion 3

2. Hovedformålet med denne artikel 5

3. Omfang, terminologi og mål 5

4. CBDC's hovedkomponenter og designvalg 6

5. Generelle privatlivsrisici og relevant rådgivning 8

5.1. Profilering og overvågning 9

5.2. Cybersikkerhedsrisici 11

5.3. Uklare roller og ansvarsområder inden for databeskyttelse 13

5.4. Finansiel udelukkelse for specifikke personer og sårbare grupper 14

5.5 Samlet vedtagelse og anvendelse af en CBDC: nødvendighed og proportionalitet 15

6. Privatlivsrisici ved visse specifikke valg eller komponenter 17

6.1. Brugen af distribueret ledgerteknologi (DLT) 17

6.2. CBDC-programmerbarhed 20

7. Argumenter for peer-to-peer online og offline betalinger 23

8. Yderligere læsning 25

[1] *Dette dokument blev drøftet på det 71. IWGDTP-møde den 7. - 8. juni 2023 og vedtaget efter endelig diskussion på det 72. IWGDPT-møde den 7.-8. december 2023. Den skriftlige procedure fulgte efter sidstnævnte møde.*

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

Resumé

En centralbanks digital valuta (CBDC) er en "fiat"2 digital valuta udstedt og bakket op af en centralbank. Størstedelen af centralbanker verden over har i det mindste forsket i CBDC, og flere er gået videre til pilotprogrammer eller endda udrulning. Blandt de fremførte årsager til en CBDC er en styrkelse af centralbankernes rolle, en styrkelse af pengepolitikken, en forbedring af finansielt tilsyn og stabilitet samt fremme af...
egen valuta.

CBDC'er udstedes af en central myndighed og er, som den traditionelle valuta, underlagt love og andre gældende regler. CBDC'er er designet til at blive brugt som en digital version af traditionel valuta, typisk til både offline (kontant) og online transaktioner, og kan understøtte nye anvendelsesscenarier, der kan påvirke enkeltpersoner og samfundet.

Hvis der ikke er tilstrækkelig beskyttelse af privatlivets fred, kontroller og sikkerhedsforanstaltninger på plads, kan CBDC'er give involverede finansielle enheder, såsom centralbanker og kommercielle banker, hidtil uset adgang til deres borgeres finansielle oplysninger. Dette ville indebære dyb indsigt i forbrugernes liv, både online og offline, hvilket muliggør profilering og overvågning af enkeltpersoner. Denne artikel tager højde for disse designvalg og identificerer de vigtigste privatlivsrisici og -udfordringer forbundet med CBDC'er ved at trække på en stikprøve af use cases; isolerer og fremhæver hovedelementerne i disse risici; og foreslår nogle overordnede råd til at afbøde disse risici. Målgruppen er interessenter såsom politiske beslutningstagere, centralbanker og andre finansielle aktører og organisationer.

Etablering af en CBDC er en kritisk beslutning, der skal tage hensyn til både fordele og omkostninger, ikke kun i betragtning af økonomiske aspekter, men også eventuelle skadelige konsekvenser for samfundet og individets rettigheder. Det kræver en omhyggelig vurdering for at undgå unødvendig og uforholdsmæssig indblanding i grundlæggende rettigheder, herunder privatlivets fred og beskyttelse af personoplysninger, men også individuel og samfundsrelateret diskrimination og økonomisk udstødelse. Implementering af en CBDC bør ikke udelukkende være drevet af ønsket om at holde trit med teknologiske tendenser eller konkurrere med andre digitale valutaer. Medmindre der er et klart og dokumenteret behov for en CBDC, vil risiciene for privatlivets fred og databeskyttelse opveje fordelene ved at oprette en CBDC.

Udformningen af CBDC'en bør være drevet af en tilgang til beskyttelse af privatlivets fred og databeskyttelse gennem design og som standard. En konsekvensanalyse af privatlivets fred og databeskyttelse, der også tager højde for bredere konsekvenser for grundlæggende rettigheder, bør udføres i planlægningsfaserne og overvåges under implementering og drift. Databeskyttelsesroller, især i anvendelsessager, hvor mange interessenter intervenerer, bør klart tildeles for at tildele rettigheder til beskyttelse af privatlivets fred og databeskyttelse.

De mulige designmuligheder for en CBDC påvirker i høj grad de resulterende privatlivs- og databeskyttelsesrisici og kræver derfor omhyggelig planlægning og vurdering fra starten. I teorien er det muligt at udvikle disintermedierede, sikre og fortrolige digitale betalinger, samtidig med at betaleren står ansvarlig.

[2] Fiatpenge er en type valuta, der er erklæret lovligt betalingsmiddel af et land, men som ikke har nogen iboende eller fast værdi. og er ikke bakket op af håndgribelige aktiver, såsom guld eller sølv.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

over for betalingsmodtageren. Anonyme betalinger ville dog være uforenelige med eksisterende lovbestemmelser, der omhandler risici for enkeltpersoner og samfundet, såsom forebyggelse af hvidvaskning af penge, bekæmpelse af terrorfinansiering og stop af skatteunddragelse. Derfor kan privatlivsfremmende teknologier bruges til at sikre ansvarlighed, samtidig med at videregivelsen af personoplysninger minimeres. Sammen med et passende design baseret på specifikke risikoprofiler er det muligt at minimere synligheden af transaktioner, der er afhængige af CBDC'er, og i stedet fokusere på de transaktioner, der bærer betydelige risici.

Andre designvalg kan bidrage til at mindske risici. Peer-to-peer- og offline-transaktioner ville forbedre beskyttelsen af privatlivets fred ved at undgå formidling, hvor det er muligt, gennem design. Behovet for programmerbare penge bør nøje vurderes i forhold til mulige negative økonomiske konsekvenser for enkeltpersoner. Begrundelsen for brugen af distribuerede ledgerteknologier bør vurderes i forhold til relevante risici, og hvis det bekræftes, bør der indføres afbødende foranstaltninger. En målrettet cybersikkerhedsramme, der spænder fra offline-anvendelsessager til interoperabilitetskrav, kan bidrage til at undgå eller afbøde virkningen af kompromitteringer af en så kritisk funktion for enkeltpersoner og samfundet.

1. Introduktion

1. Fremkomsten af digitale centralbankvalutaer (CBDC'er) repræsenterer et banebrydende skift for det globale finansielle system. Private kryptovalutaer har allerede påvirket den måde, folk engagerer sig i finansielle transaktioner på. Fortalere hævder, at private kryptovalutaer øger inklusion og gennemsigtighed, fremskynder transaktioner og reducerer omkostninger, selvom størstedelen af disse fordele ikke er blevet til noget.3 I mellemtiden har nuværende kryptovalutaer en negativ indvirkning på miljøet samt større risici, såsom dem, der er forbundet med karakteren af normalt uregulerede valutaer, herunder høj volatilitet, sårbarhed over for svindel og værditab. CBDC'er har potentiale til at transformere, hvordan digital valuta udstedes, distribueres og bruges på globalt plan. Størstedelen af centralbanker verden over4 har i det mindste forsket i digital centralbankvaluta, hvoraf flere er gået videre til pilotprogrammer eller lancerer CBDC'er. Dette kommer som reaktion på den øgede anvendelse af digitale, kontaktløse betalinger, kryptovalutaer og e-handel,5 som yderligere er accelereret af Covid-19. Væksten er også ansporet af de muligheder, som disse digitale valutaer tilbyder som et mere fleksibelt monetært værktøj sammenlignet med eksisterende ikke-digital valuta.

2. En CBDC er en "fiat" digital valuta udstedt og bakket op af en centralbank. I modsætning til kryptovalutaer som Bitcoin udstedes CBDC'er af en central myndighed og er, ligesom den traditionelle valuta, underlagt love og andre gældende regler. CBDC'er er designet til at blive brugt som en digital version af

[3] Det amerikanske finansministerium, kryptoaktiver: Implikationer for forbrugere, investorer og virksomheder som 44-årig (september) 2022). Tilgængelig på: https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

[4] https://www.atlanticcouncil.org/cbdctracker og https://cbdctracker.org Den Europæiske

[5] Centralbank: Undersøgelse af forbrugernes betalingsadfærd i euroområdet (SPACE) – 2022. Tilgængelig på: https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

traditionel valuta, typisk til både offline- og onlinetransaktioner, og kan understøtte nye anvendelsesscenarier6 , der kan påvirke enkeltpersoner og samfundet.

3. Udformningen af en CBDC kan variere betydeligt afhængigt af hver jurisdiktion's vurdering af, hvordan en CBDC kan understøtte offentlige politiske mål. Mens nogle få CBDC'er allerede er i drift, er mange andre stadig i forskningsfasen, under planlægning, udvikling eller testning, og nogle få er allerede blevet afviklet. Fremtidige og eksisterende CBDC'er kan blive ændret i takt med at teknologien og det regulatoriske landskab udvikler sig.

4. Centralbanker har fremført mange grunde til at anvende deres CBDC.7 For det første er der centralbankernes styrkede rolle i det globale finansielle system. CBDC'er kan påvirke dette på flere måder.8 For det første kan CBDC'er styrke pengepolitikken ved at give centralbankerne yderligere værktøjer til at implementere politikken mere præcist og effektivt. For det andet kan CBDC'er fremme finansiel stabilitet ved at tilbyde et sikrere betalingsmiddel og reducere risikoen for værditab for brugerne i tilfælde af bankrus.9 Derudover kan CBDC'er bidrage til at informere udformningen af økonomisk politik samt forbedre de finansielle tilsynskapaciteter ved at give centralbankerne en bedre forståelse af, hvordan penge bruges, og hvor de opbevares. Endelig kan CBDC'er fremme national suverænitet ved at give regeringer mulighed for at opretholde kontrollen over deres pengepolitik over private enheder eller udenlandske regeringer.

5. En anden grund til, at en centralbank udsteder en CBDC, er at hjælpe med at styrke sin egen valuta. Oprettelsen af en CBDC kunne øge markedets tillid til den valuta, der udstedes i den pågældende jurisdiktion, da det ville repræsentere en konkret forpligtelse fra centralbanken til at sikre finansiel stabilitet. Derudover ville udstedelse af en CBDC give centralbanken et nyt middel til at fremme brugen af den nationale valuta, hvilket potentielt ville reducere afhængigheden af andre valutaer og styrke den nationale valutas position i det globale finansielle system.

6. Fra et privatlivs- og databeskyttelsesperspektiv, som allerede beskrevet af EDPS i nyere arbejde,10 CBDC'er kan give regeringer, centralbanker og involverede finansielle enheder hidtil uset adgang til deres borgeres finansielle oplysninger, hvilket udgør en betydelig risiko for privatlivets fred.

---

[6] Såsom programmerbare betalinger og penge, som illustreret senere i teksten.
[7] For en omfattende analyse af mål og årsager, se Bank for International Settlements, BIS Papers No 125, Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies, af Anneke Kosse og Ilaria Mattei, maj 2022.
[8] For yderligere information, se https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2713~91ddff9e7c.en.pdf
[9] Et bankrun er en situation, hvor mange kunder samtidig hæver deres indskud fra en bank på grund af bekymringer om bankens solvens eller stabilitet. Dette kan føre til en likviditetskrise for banken, hvilket gør det vanskeligt for den at imødekomme sine indskyderes krav og potentielt kan føre til bankens konkurs. For mere information, se Allen, F. & Gale, D. (2000). Financial contagion. Journal of Political Economy, 108(1), 1-33. https://doi.org/10.1086/262109
10https ://edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-03-29-techdispatch-12023-central-bank-digital-currency_en

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

sikkerhed og individers rettigheder. I betragtning af den igangværende tendens i mange lande til gradvist at opgive brugen af kontanter, som i sagens natur er langt mindre sporbar end digitale transaktioner, ville CBDC'er være de naturlige kandidater til at erstatte den. Derfor skal CBDC's funktioner og design vurderes nøje, når man planlægger dens gennemførlighed.11 Privatliv og beskyttelse af rettigheder og friheder skal indbygges i designet fra starten for at skabe en troværdig CBDC.

2. Hovedformålet med dette dokument

7. I de seneste par år har eksperter skrevet udførligt om, hvordan privatlivskrav vil påvirke planerne for CBDC'er. Der er blevet foreslået et par løsninger, som skal tilpasses de komplekse politiske, operationelle og teknologiske muligheder. Centralbanker og interessenter har også fremsat adskillige overvejelser om, hvordan man designer en privatlivsbeskyttende CBDC. Målene med denne artikel er (i) at identificere de vigtigste privatlivsrisici og -udfordringer forbundet med CBDC'er, ud fra en stikprøve af use cases identificeret i vores forskning, (ii) at isolere og fremhæve hovedelementerne i disse risici, og (iii) at foreslå nogle overordnede råd for at afbøde risiciene og sikre, at CBDC'er designes og implementeres på en måde, der respekterer borgernes privatliv og rettigheder.

3. Omfang, terminologi og mål

8. CBDC'er kan groft opdeles i to kategorier: detailhandel og engroshandel. Detail-CBDC'er er designet til offentlig brug og har normalt til formål at supplere eller erstatte nuværende detailbetalingsmetoder, såsom kontanter, checks, betalingskort osv. Engros-CBDC'er er derimod designet til brug for centralbanker og finansielle institutioner og har til formål at lette interbankbetalinger og -afvikling.

9. Denne artikel fokuserer på CBDC'er i detailhandlen på grund af deres direkte indvirkning på enkeltpersoners privatliv. Engros-CBDC'er falder uden for denne artikels omfang.

10. Dette dokument henvender sig primært til interessenter som beslutningstagere, centralbanker og andre finansielle aktører og organisationer for at opfordre dem til at tage hensyn til privatlivets fred og individuelle rettigheder, når de udarbejder CBDC'er. Offentligheden, der vil bruge CBDC'en til betalinger, og civilsamfundsorganisationer, der forsvarer folks rettigheder og friheder, kan også drage fordel af det for at forstå udfordringerne og være i stand til korrekt at vurdere risiciene ved de tilbudte CBDC'er.

[11] Den Internationale Valutafond har udsendt et dokument, der foreslår "en dynamisk beslutningsramme, hvorunder centralbanken kan træffe beslutninger under usikkerhed" med henblik på en CBDC. G. Soderberg et al., Hvordan bør centralbanker udforske centralbankers digitale valuta?, 8. september 2023. Tilgængelig på: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504 Privatliv er blandt de elementer, der tages i betragtning, på side 21.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

4. CBDC's hovedkomponenter og designvalg

11. For at kunne foretage en faktuel analyse af risici skal vi først klart identificere de vigtigste funktionelle byggesten (som vi vil kalde "komponenter"), der forventes i en CBDC. Selvom CBDC-strukturen kan variere, vil denne artikel fokusere på et par hovedkomponenter, der ses mest konsekvent i CBDC-projekter fra centralbanker over hele verden, og som samtidig har mærkbare udfordringer med hensyn til privatlivets fred. Dette vil give indsigt i de forskellige måder, de kan designes og implementeres på, og hvilken indvirkning dette har på privatlivsrisici og deres afbødning.

12. Baseret på vores observation følger en liste over hovedkomponenterne i CBDC-projekter. Nogle af dem er funktionelle for andre, mens andre kan betragtes som delkomponenter eller horisontale processer. Ikke alle disse komponenter er strengt nødvendige for et CBDC-system, men regeringer forsøger generelt at implementere dem alle. Som regel vil vi ikke gennemgå hver komponent i denne artikel, men det kan være nyttigt at have dem på listen til yderligere, mere specifik analyse.

Identitetsstyring: et system til verifikation og styring af brugeridentiteter, typisk involverende digitale identifikationsmetoder og autentificerings- og autorisationsprotokoller.

Onboarding: processen med at registrere og integrere nye brugere i CBDC-systemet, herunder Know Your Customer (KYC)12- tjek og oprettelse af digitale tegnebøger13 eller konti.

• Værdilagring: en digital repræsentation af valutaens værdi, som kan opbevares digitalt tokens eller konti, der forvaltes af finansielle institutioner eller centralbanken.

• Værdioverførsel (betalinger): mekanismer og protokoller til overførsel af værdi mellem parter, hvilket kan involvere peer-to-peer-transaktioner eller formidlere såsom banker.

o Transaktionsstyring: et system til behandling, validering og registrering af transaktioner, som kan være baseret på centraliserede eller decentraliserede ledgerteknologier.

o Offlinebetalinger: muligheden for, at den digitale valuta kan transageres og bruges til betalinger uden brug af en internetforbindelse.

o Peer-to-peer-betalinger: en funktion, der muliggør direkte transaktioner mellem brugere uden behov for mellemmænd, og som udnytter CBDC'ens transaktionsstyrings- og værdioverførselskomponenter.

[12] KYC-procedurer er en afgørende del af effektiv håndtering af risici for hvidvaskning af penge og finansiering af terrorisme. KYC-foranstaltninger hjælper virksomheder med at forstå deres kunder og deres økonomiske transaktioner og med at opdage mistænkelige aktiviteter. For mere information, se https://en.wikipedia.org/wiki/Know_your_customer

[13] Dette udtryk kan omfatte enheder såsom smartkort, der også kan bruges til offlinebetalinger eller mobilapps til onlinebetalinger.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

- o Afviklingsproces: processen med at færdiggøre transaktioner, sikre at værdioverførslen er gennemført og uigenkaldelig, og opdatere de involverede parters saldi.
- o Interoperabilitet i betalinger: muligheden for at interagere med CBDC-systemet under andre jurisdiktioner for at muliggøre grænseoverskridende betalinger.

• Programmerbarhed af betalinger og penge: system til automatisering af betalingsprocesser på bestemte tidspunkter og udvikling af nye finansielle produkter og tjenester gennem smarte kontrakter14 og andre programmerbare funktioner.

• Anti-hvidvaskning af penge (AML) og generel svindelhåndtering: systemer og værktøjer til at opdage, forebygge og reagere på potentielt svigagtige aktiviteter, såsom uautoriserede transaktioner, identitetstyveri og anden ondsindet adfærd.

• Kontogendannelse: systemer, der giver enkeltpersoner mulighed for at få penge eller relaterede digitale identiteter tilbage i scenarier, hvor personen skifter elektronisk enhed, bliver offer for svindel, mister kontooplysninger eller overfører konti, når personen dør.

• Pengepolitiske værktøjer og mekanismer: Disse kan omfatte værktøjer eller mekanismer, der anvendes til at styre beholdningsgrænser og relaterede nødmekanismer (såsom ombytning af kreditorer).

13. De mulige designvalg for en CBDC har en dybtgående indvirkning på de deraf følgende privatlivs- og databeskyttelsesrisici. Trods de mange mulige CBDC-designdimensioner kan vi identificere tre som de mest betydningsfulde: valget af CBDC'ens driftsmodel, den underliggende IT-infrastrukturmodel og den måde, hvorpå brugerens autorisation til at udføre CBDC-operationer verificeres. Disse designvalg har vigtige konsekvenser for CBDC'ens funktionalitet, sikkerhed og privatliv.15 Måden, de er kategoriseret nedenfor, hjælper med at afklare de problemstillinger, der står på spil, og bredden af muligheder.

14. En CBDC-modeltype kan være **direkte, indirekte eller en hybrid** af de to (også kaldet henholdsvis en-lags, to-lags eller en hybrid tilgang). I en direkte model driver centralbanken den samlede CBDC fuldt ud, opbevarer brugerkonti og administrerer alle funktionelle komponenter i CBDC'en. Denne mulighed forkastes normalt, da den fuldstændigt ville revolutionere det nuværende system, lægge byrder og ansvar på centralbankerne, samtidig med at formidlernes rolle drastisk reduceres. I en indirekte model ville centralbanken delegere de fleste operationelle opgaver til de finansielle formidlere, såsom brugeronboarding, administration af brugerkonti og bekæmpelse af hvidvaskning af penge/bekæmpelse af...

---

[14] En smart kontrakt er en selvudførende digital kontrakt, der indeholder vilkårene i en aftale mellem parterne skrevet direkte i kodelinjer. Koden er lagret på et blockchain-netværk, hvilket sikrer dens udførelse og håndhævelse uden behov for mellemled. For mere information, se Antonopoulos, AM (2014).
Mestring af Bitcoin: Lås op for digitale kryptovalutaer. O'Reilly Media.

[15] Se for eksempel: Tsang, Cheng-Yun (CY) og Yang, Alex Yueh-Ping og Chen, Ping-Kuei, Disciplining CBDCs: Addressing the Privacy Aspects and Central Bank Independence (20. oktober 2022), tilgængelig på SSRN: https://ssrn.com/abstract=4253888 eller http://dx.doi.org/10.2139/ssrn.4253888, og Pocher, Nadia og Veneris, Andreas, Privatliv og gennemsigtighed i CBDC'er: En reguleringsbaseret AML/CFT-ordning (3. januar 2021). Tilgængelig på SSRN: https://ssrn.com/abstract=3759144 eller http://dx.doi.org/10.2139/ssrn.3759144.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

finansiering af terrorisme (AML/CFT). En hybrid CBDC ville kombinere elementer fra begge tilgange. For eksempel kan centralbanker enten opbevare en kopi af alle detailtransaktioner eller blot administrere engrosbalancer med formidlere. Derudover kan de fortsætte med at delegere afviklingen af detailbetalinger til formidlere eller udføre direkte afvikling af alle transaktioner.

15. CBDC's IT-infrastrukturmodeller kan enten benytte en **centraliseret** ledger/arkiv eller en **distribueret** ledger (DLT). I den centraliserede model registreres alle brugertransaktioner i en central ledger under centralbankkontrol. I den distribuerede model bemyndiger centralbankerne et begrænset antal andre enheder til at opdatere ledgeren. Uanset valget kræver selve CBDC'ens natur, at centralbanken opretholder rollen som central myndighed og et højt niveau af kontrol over ledgeren, herunder over størrelsen af den udstedte CBDC, hvem der kan opdatere ledgeren og andre elementer.

16. Endelig kan CBDC'en enten være **token- eller kontobaseret.** En tokenbaseret CBDC bruger en digital token (såsom en digital signatur) under brugernes kontrol til at få adgang til og bruge den valuta, de ejer, uden at det er nødvendigt at give nogen identitetsoplysninger, såsom en digital version af pengesedler eller mønter. En betalingsmodtager, der modtager en digital token, behøver ikke at verificere kundens identitet - kun gyldigheden af selve tokenet. Omvendt kræver en kontobaseret CBDC, at den mellemmand, som brugeren har sin konto hos, identificerer brugeren, administrerer kontoen og sporer relaterede transaktioner og saldi, som det sker, når man bruger private bankpenge på bankkonti.

5. Generelle privatlivsrisici og relevant rådgivning

17. CBDC'er indebærer adskillige udfordringer inden for privatlivets fred og databeskyttelse. En undersøgelse foretaget af Den Europæiske Centralbank16 viste, at privatliv og sikkerhed er de mest påtrængende bekymringer for europæiske borgere. Disse bekymringer er særligt relevante i betragtning af den stigende brug af digitale teknologier, den voksende betydning af personoplysninger i den moderne økonomi og de potentielle overvågningsrisici fra regeringer og private finansielle organisationer, som implementeringen af en CBDC kan medføre, hvis betalinger overvåges omfattende.

18. Potentielle konsekvenser for privatlivets fred vil først afhænge af de politiske mål og karakteristika17 i CBDC. En klar specifikation af disse mål og planlagte funktionaliteter, samt af det mulige samspil med andre digitale og finansielle elementer og politiske initiativer, er afgørende for at kunne vurdere disse konsekvenser. Desuden kræver sikring af privatlivets fred passende designvalg ved nøje at overveje de planlagte CBDC-designvalg for dens komponenter, såsom identitetsstyring, transaktions- og afviklingsstyringssystemet samt værdilagring og -opbevaring.

[16] Den Europæiske Centralbank. ECB offentliggør resultaterne af den offentlige høring om en digital euro. 2021. Tilgængelig på https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

[17] For eksempel kan en politik begrænse mængden af CBDC pr. bruger, hvor andre politikker måske ikke gør det. Valget kunne være kun at tillade én CBDC-konto pr. bruger, mens en anden mulighed er at tillade mange. Eller programmerbare penge kunne være en funktion i en CBDC, men ikke i andre.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

overførselsmekanismer. Disse valg bør være resultatet af en korrekt vurdering af privatlivsrisici, der fører til identifikation af passende afbødende foranstaltninger.

19. I teorien er det muligt at udvikle disintermedierede, sikre og fortrolige digitale betalinger, der sikrer betalers ansvarlighed over for betalingsmodtageren. Anonyme betalinger ville dog være uforenelige med eksisterende lovbestemmelser, der omhandler risici for enkeltpersoner og samfundet og pålægger visse databehandlingsaktiviteter i den finansielle sektor. For eksempel stiller love, der har til formål at forhindre hvidvaskning af penge, bekæmpe finansiering af terrorisme og stoppe skatteunddragelse, specifikke krav, der nødvendiggør behandling af personoplysninger (såsom betalers/modtagers identitet, betalingshistorik, saldi) af kompetente myndigheder med adgang til data. Designet og funktionerne i en CBDC kan tage hensyn til specifikke risikoprofiler vedrørende bekæmpelse af hvidvaskning af penge og terrorfinansiering for at undgå fuld synlighed af transaktioner, der er afhængige af CBDC'er, og i stedet fokusere på dem, der repræsenterer betydelige risici.

5.1. Profilering og overvågning

20. Kontanter er den eneste form for fortroligt udvekslede offentlige penge, der opererer inden for regulerede områder. Den øgede anvendelse af digitale betalinger og reduceret brug af kontanter18 identificerer en tendens mod et fuldt digitalt betalingslandskab, hvilket kan resultere i øget udnyttelse af data om finansielle transaktioner.

21. Hvis der ikke er tilstrækkelig beskyttelse af privatlivets fred, kontrol og sikkerhedsforanstaltninger på plads, kan omfattende transaktionssporing give dybdegående indsigt i forbrugernes liv, både online og offline, hvilket muliggør profilering og overvågning af enkeltpersoner af parter involveret i betalingssystemer eller enhver anden enhed, der får adgang til dataene. En CBDC kan muliggøre overvågning af finansielle transaktioner i realtid og potentielt afsløre følsomme personlige oplysninger om enkeltpersoner, selv ud over deres forbrugsvaner, indkomst og økonomiske forpligtelser. Betalingsdata kan afsløre et fuldstændigt billede af brugernes privatliv, herunder sundhedstilstand, seksuel orientering, religiøse og filosofiske overbevisninger og politiske holdninger. Akkumulering og tilgængelighed af en så stor mængde data udgør en alvorlig risiko for de registreredes rettigheder og friheder på grund af mulig masseovervågning, diskrimination, ulovlig genbrug og databrud.

22. Udstedelse af en CBDC giver anledning til specifikke bekymringer vedrørende centralbankers, regeringers og andre offentlige myndigheders adgang til finansielle oplysninger knyttet til enkeltpersoner, hvilket introducerer risikoen for, at systemisk overvågning krænker demokratiske regler og borgernes privatliv og grundlæggende rettigheder. Denne risiko kan variere afhængigt af landets institutionelle og demokratiske opbygning og centralbankernes uafhængighedsniveau.19 Risikoen ved fysisk eller virtuel adgang til data kan potentielt udnyttes, hvis den politiske og institutionelle kontekst ændrer sig.

18 Se fodnote 5.

19 Tsang, Cheng-Yun (CY) og Yang, Alex Yueh-Ping og Chen, Ping-Kuei, Disciplinering af CBDC'er: Håndtering af privatlivsaspekterne og centralbankuafhængighed (20. oktober 2022). Vindende artikler fra DC Fintech Week 2022, tilgængelige på SSRN: https://ssrn.com/abstract=4253888 eller http://dx.doi.org/10.2139/ssrn.4253888.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Machine Translated by Google

23. I den nuværende betalingsramme er AML/CFT-operationer delegeret til finansielle formidlere. Direkte eller hybride CBDC'er ville tilføje en central AML/CFT-tjeneste, der udføres direkte eller indirekte af centralbanker. I direkte CBDC'er ville centralbanker næsten fuldstændigt overtage fra formidlere, og hybride CBDC'er kunne have forskellige mulige tjenestekonfigurationer, hvor centralbanker enten yder strategisk rådgivning ved at udnytte aggregerede data til mønsteridentifikation eller udfører AML/CFT-kontroller i realtid baseret på realtidssynlighed af CBDC-transaktioner.

Råd

24. Et CBDC-design, der begrænser adgangen for centralbanker, regeringer og andre interessenter til personlige oplysninger og prioriterer dataminimering, kan bidrage til at reducere privatlivsrisici. I modsætning hertil ville en konfiguration, der muliggør unødvendig indsamling og giver mulighed for at identificere og lagre personlige oplysninger og betalingsdata eller at linke betalingsdata til kundeprofiler, forstærke privatlivsrisici.

25. Fra et privatlivs- og databeskyttelsesperspektiv tilføjer direkte eller hybride CBDC'er, der gør det muligt for centralbanker at se alle transaktioner, en ny, specifik risiko i forhold til en indirekte CBDC, hvor en centralbank kun kan se engrostransaktioner med finansielle formidlere. I en indirekte CBDC-modalitet ville betalingsdata kun være synlige for finansielle formidlere, hvilket udgør en privatlivsrisiko, der kan sammenlignes med den, der følger af brugen af debet- og kreditkort i kontobaserede digitale betalingssystemer, hvor private banker ulovligt kan behandle en kontohavers personoplysninger.

26. Hvor designet giver centralbanker mulighed for at se transaktioner, kan privatlivsfremmende teknologier (PET'er) tilbyde værktøjer til at mindske risici. For eksempel ville pseudonymiseringsteknikker ikke afsløre brugernes reelle identitet for centralbanker, men ville stadig give dem mulighed for at foretage vurderinger af transaktioner baseret på pseudonymet. Denne beskyttelse ville kræve andre juridiske og organisatoriske foranstaltninger for at sikre et rimeligt beskyttelsesniveau for at undgå ulovlig centralbankers adgang til identifikationsdata, der opbevares af formidlere, og sætte grænser for genidentifikation.

27. For at sikre ansvarlighed og samarbejde, samtidig med at videregivelse af personoplysninger til centralbanker og formidlere minimeres, anvendes mere avancerede PET'er,20 såsom nulvidensbeviser21, herunder Pedersen-forpligtelser,22 engangsadresser,23 homomorf kryptering, flerpartskryptering

[20] ENISA kalder dem «avancerede pseudonymiseringsteknikker». Se ENISA, januar 2001, Data Avancerede teknikker og anvendelsesscenarier til pseudonymisering. Findes på: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/

[21] Gross, Jonas og Sedlmeir, Johannes og Babel, Matthias og Babel, Matthias og Bechtel, Alexander og Schellinger, Benjamin, Design af en digital centralbankvaluta med understøttelse af kontantlignende privatliv (22. juli 2021). Tilgængelig på SSRN: https://ssrn.com/abstract=3891121 eller http://dx.doi.org/10.2139/ssrn.3891121.

[22] Id.

[23] Den Europæiske Centralbank, Bank of Japan, februar 2020, STELLA – fælles forskningsprojekt for Den Europæiske Centralbank Centralbanken og Bank of Japan, Balancering af fortrolighed og revisionsbarhed i en distribueret hovedbog

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

beregning24 osv. kan implementeres. Forskningsprojekter og pilotimplementeringer25 er veletablerede og giver angiveligt mulighed for alt fra definitiv anonymitet i betalinger26 til delvis/tilbagekaldelig anonymitet27 under hensyntagen til forskellige niveauer af ansvarlighed og behov for revisionsbarhed. Brugen af disse PET'er skal sameksistere med andre krav såsom ydeevne, skalerbarhed, brugervenlighed og tilgængelige ressourcer samt integration med eksisterende betalingsinfrastruktur,28 hvilket repræsenterer en af de største designudfordringer.

28. Betalingsfortrolighed under en bestemt betalingstærskel (under hensyntagen til AML/CFT-risici) kan også være en hidtil uset privatlivsfokuseret funktion for CBDC-løsninger, der adskiller den fra andre private digitale betalingsmetoder, der anvendes af borgere, hvor anonyme kontantløse betalinger ikke er en mulighed. Der kan indføres transaktionslofter, der gør det muligt at afblindne eller deanonymisere en transaktion over en bestemt tærskel. Sådanne lofter kan være en mere privatlivsbeskyttende tilgang til kontrol mod hvidvaskning af penge end udbredte krav til transaktionsrapportering, mønsteranalyse af små transaktioner eller andre overvågningsfunktioner i realtid29. Peer-to-peer-betalinger og offline-betalinger (se nedenfor for mere fokus) er også privilegerede designvalg for at minimere datadeling.

29. Personoplysninger vedrørende CBDC-operationer bør kun behandles i den periode, der er nødvendig for at udføre identificerede nødvendige og lovlige operationer. Efter denne periode bør de slettes eller anonymiseres og ikke længere være tilgængelige for andre interessenter end betaler og betalingsmodtager.
Lovgivere bør definere specifikke opbevaringsperioder for personoplysninger baseret på formålet med databehandlingen. Dette ville reducere mængden af tilgængelige data og risikoen for profilering, overvågning og brug på datasikkerheden.

5.2. Cybersikkerhedsrisici

30. For at etablere den tillid, som borgerne skal have for at føle sig trygge ved at indføre og bruge CBDC'er, skal der være høj sikkerhed på plads. CBDC'er er afhængige af kompleks digital infrastruktur og datalagring.

---

miljø. Tilgængelig på: https://
www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf.

[24] Se afsnit 3.1.2 i Bank of Japan, Central Bank Digital Currency Experiments Results and Findings from Proof of Concept Phase 2, maj 2003. Tilgængelig på: https://www.boj.or.jp/en/paym/digital/dig230529a.pdf

[25] Id.

[26] D. Chaum. Blinde underskrifter for usporbare betalinger. I Crypto '82, Plenum Press NY, 1983.

[27] J. Claessens, B. Preneel, J. Vanderwalle. Anonymitetsstyrede elektroniske betalingssystemer, 1999. Tilgængelig på: https://www.esat.kuleuven.be/cosic/publications/article-360.pdf.

[28] Auer, Raphael og Böhme, Rainer, Teknologien bag digitale valutaer i detailcentralbanker (1. marts 2020). BIS Quarterly Review, marts 2020, tilgængelig på SSRN: https://ssrn.com/abstract=3561198.

[29] David Chaum, Christian Grothoff og Thomas Moser, Sådan udsteder du en digital centralbankvaluta, SNB Arbejdspapirer (marts 2021), https://www.snb.ch/en/publications/research/working-papers/2021/working_paper_2021_03 .

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

systemer og kan være sårbare over for cyberangreb30 , der kan kompromittere brugernes økonomiske sikkerhed og privatliv samt økonomien i stor skala. Sikkerhedsproblemer i CBDC-infrastrukturen kan få alvorlige konsekvenser blandt interessenter og et betydeligt tab af tillid fra brugerne, hvilket kan føre til, at de afviser CBDC som en levedygtig betalingsmulighed, hvilket resulterer i projektets fiasko.
For nylig har behovet for at sikre cybersikkerhed inden for CBDC fået mere fokus31, og der udvikles målrettede cybersikkerhedsrammer32.

31. Visse risici, der er almindelige i eksisterende betalingssystemer, er også værd at bemærke for CBDC'er. Uautoriseret adgang til legitimationsoplysninger kan kompromittere brugerkonti og personoplysninger, der behandles for en CBDC. Cyberangribere anvender sofistikerede teknikker som social engineering, sidekanalangreb og malware til at udtrække legitimationsoplysninger fra brugernes enheder, hvilket kan føre til potentielt forstyrrende konsekvenser.

32. Desuden udgør den eksponentielle stigning i computerkraft som følge af fremkomsten af kvantecomputere en potentiel trussel mod sikkerheden i finansielle tjenester. Kvantecomputere er i stand til at kompromittere nogle eksisterende datakrypteringsmetoder og kryptografiske primitiver, der i øjeblikket beskytter adgangen, fortroligheden og integriteten af lagrede og transmitterede data.

33. En anden kritisk sikkerhedsrisiko er koncentrationen af betalingsdata, almindeligvis omtalt som "datakoncentration". Hvis alle CBDC-brugeres betalingsdata blev lagret i en centralbanks databaser, ville det skabe attraktive incitamenter til cyberangreb og udgøre en høj systemisk risiko. Databrud eller ulovlig adgang til disse koncentrerede data kan resultere i individuel eller generel udbredt overvågning, tab af midler, bedrageri og andre skader på privatlivets fred og individuelle rettigheder. Derudover kan muligheden for denial-of-service-angreb rettet mod en centraliseret database forstyrre alle betalingsoperationer.

34. Alternativt, hvor en distribueret arkitektur/teknologi implementeres, og især hvor data lagres på brugerenheder, bliver det afgørende effektivt at minimere risiciene forbundet med "double-spending"-angreb, især i den offline, bearer-baserede konfiguration af en CBDC.
Disse angreb involverer ulovlig brug af CBDC flere gange, en form for forfalskning.

35. Desuden kan der, selvom CBDC'er normalt er knyttet til en specifik jurisdiktion, opstå risici som følge af interoperabilitet og grænseoverskridende dimensioner33 . Da centralbanker primært fokuserer på indenlandske CBDC-applikationer, kan der blive givet utilstrækkelig opmærksomhed til grænseoverskridende regulering, interoperabilitet og

[30] The Guardian. (2021). New Zealands centralbank siger, at dens systemer er blevet hacket. Findes på: https://www.theguardian.com/world/2021/jan/11/new-zealands-central-bank-says-its-systems-have-been-hacked

[31] For yderligere information se Atlantic Council, Manglende nøgle: udfordringen med cybersikkerhed og centralbank digital valuta, juni 2022 - tilgængelig på https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/ .

[32] BIS Innovation HUB, Project Polaris: et sikkerheds- og robusthedsrammeværk for CBDC-systemer. Tilgængelig på: https://www.bis.org/publ/othp70.htm.

[33] Igangværende pilotprojekter kan bidrage til at øge bevidstheden, også om interoperabilitetsrelaterede privatlivsspørgsmål. Se f.eks. BIS Innovation HUB, Project Icebreaker: breaking new paths in cross-border retail CBDC payments, især afsnit 6.6. Findes på: https://www.bis.org/publ/othp61.htm

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

standardisering. Overførsel af person- og transaktionsdata på tværs af flere jurisdiktioner kan også forstærke omfanget, omfanget og hastigheden af potentielle databrud.

Råd

36. Da CBDC'er ville være afgørende for mennesker og økonomier, skal de have veldefinerede og stærke sikkerhedsstyrings- og risikostyringsprocesser, herunder vedtagelse af robuste sikkerhedsforanstaltninger for at beskytte CBDC-infrastrukturen, beskytte brugeraktiver og data og sikre modstandsdygtighed over for cyberangreb. Generelt er cybersikkerhed for bank- og betalingstjenester allerede stærkt reguleret og juridisk obligatorisk i nogle jurisdiktioner.

37. Samarbejde mellem cybersikkerhedsaktører er afgørende for at afbøde relevante risici og harmonisere cybersikkerhedsrammer. Dette muliggør lige vilkår og sikrer mere sikker interoperabilitet uden svage led. Der skal fastsættes internationale standarder under hensyntagen til de minimumssikkerhedsforanstaltninger, som CBDC'er skal overholde.

38. Der bør lægges særlig og kontinuerlig vægt på vurdering af teknologier og algoritmer. Open source-løsninger ville være særligt nyttige for at muliggøre gennemsigtighed og peer review, forudsat at der vedtages og implementeres en tilstrækkelig open source-styring og -administration inden for CBDC-projektet. Adoption af open source ville også fremme inklusion og offentlig opbakning.

39. Ved design af CBDC-teknologier skal postkvantekryptografi tages i betragtning, da det kan modstå kvantesystemers computerkraft og give forbedrede sikkerhedsforanstaltninger. Centralbanker, der foreslår CBDC'er, bør identificere en fælles tilgang[34] .

5.3. Uklare roller og ansvarsområder inden for databeskyttelse

40. Baseret på de specifikke designvalg, som centralbanken foretager, kan forskellige aktører (centralbanker, regeringen, formidlere, private virksomheder, der fungerer som leverandører) inden for CBDC-økosystemet være involveret i behandling af personoplysninger. Det er afgørende at anerkende de forskellige databeskyttelsesroller, som disse aktører spiller for at sikre overholdelse af gældende love og sikre, at enkeltpersoner effektivt kan udøve deres databeskyttelsesrettigheder. Især ved implementering af en decentraliseret arkitektur, såsom dem, der er baseret på Distributed Ledger Technology (DLT)[35], kan forvaltningsstrukturen og involveringen af flere aktører i databehandlingen præsentere specifikke udfordringer.

Råd

41. Identificer ansvarsområder baseret på gældende databeskyttelseslovgivning (f.eks. dataansvarlig(e) og databehandler(e) i GDPR) for at tildele ansvarlighed og forpligtelser i hele betalingen

[34] BIS Innovation HUB, Projekt Leap: kvantesikring af det finansielle system. Tilgængelig på: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.

[35] Se afsnit 6.1

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

kæden og andre tilknyttede finansielle operationer. Det er afgørende at etablere en klar styring og opgavefordeling mellem centralbanker og finansielle formidlere for at fastlægge databeskyttelsesforpligtelser i et decentraliseret miljø med flere parter, for eksempel hvilken enhed der er ansvarlig for underretning om et potentielt brud på persondatasikkerheden eller for at håndtere de registreredes rettigheder, såsom retten til information, adgang eller tilbagetrækning af samtykke.

42. Etabler klare kommunikationskanaler og samarbejds- og koordineringsmekanismer. Dette omfatter datadelingsaftaler og implementeringsforanstaltninger for at sikre, at de registreredes rettigheder respekteres i hele CBDC's funktion, lige fra onboardingfasen. Samarbejdsindsatser er afgørende for at imødegå de udfordringer, der er forbundet med databeskyttelse i en så kompleks kontekst.

5.4. Finansiel udelukkelse for specifikke personer og sårbare grupper

43. 40. En CBDC vil ikke automatisk øge den finansielle inklusion. Hvorvidt en digital valuta giver mennesker i samfundets udkant mere adgang til det finansielle system eller forværrer eksisterende kløfter, er et spørgsmål om CBDC's design, implementering og den sociale støtte, der ydes til at onboarde mere marginaliserede brugere.36 En dårligt designet CBDC risikerer at udelade mennesker med mindre teknisk forståelse, mennesker uden pålidelig internetadgang, fattige samfund og papirløse/ migrantsamfund. Hvis CBDC parres med reduktion eller eliminering af fysiske kontanter, kan konsekvenserne for allerede marginaliserede befolkningsgrupper være alvorlige. Finansiel udstødelse falder i to kategorier, der bør behandles separat: utilsigtet udstødelse og forsætlig udstødelse gennem statslig undertrykkelse.

44. Utilsigtet udelukkelse omfatter dårlige designvalg, der gør en CBDC utilgængelig for den gennemsnitlige bruger eller marginaliserede befolkningsgrupper. For eksempel er det usandsynligt, at en CBDC, der er fuldt formidlet af det eksisterende banksystem, vil øge den økonomiske inklusion for personer, der i øjeblikket ikke har tillid til bankerne og nægter eller nægtes adgang til bankvirksomhed. I modsætning hertil kan en tokeniseret CBDC, der kan opbevares i en hvilken som helst digital tegnebog, øge den økonomiske inklusion ved at fremme onlinetransaktioner for personer uden bankforbindelse.

45. Utilsigtet udelukkelse kan også skyldes dårlig politik omkring CBDC'er. Mindre teknisk kyndige befolkningsgrupper som ældre personer og potentielt personer i landdistrikter vil muligvis ikke automatisk indføre en CBDC uden social støtte og inkluderende design. Det samme gælder for personer med handicap, der interagerer anderledes med deres smartphones.

46. Bevidst finansiel udelukkelse kan skyldes specifikke beslutninger truffet af regeringer om at nægte visse individer eller endda visse grupper og befolkningsgrupper adgang til CBDC'er, med en stærk indvirkning på individets rettigheder og friheder, samt begrænsninger for specifikke anvendelser. En sådan udelukkelse kan også formuleres i form af terrorbekæmpelse eller hvidvaskningsindsatser, der falder ind under

[36] Ashley Lanquist og Brandon Tan, Centralbankernes digitale valutas rolle i at fremme finansiel inklusion, Den Internationale Valutafond Fintech Notes (september 2023), https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/22/Central-Bank-Digital-Currency-s-Role-in-Promoting-Financial-Inclusion-538728 .

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Machine Translated by Google

uforholdsmæssigt hårdt ramme minoritetsbefolkninger eller være mere eksplicit målrettet etniske/religiøse minoriteter eller indvandrere 37. Systemer, der giver regeringer mulighed for at afskære adgangen til en CBDC for enkeltpersoner eller befolkningsgrupper, skaber større risiko for økonomisk udelukkelse end systemer, der behandler en CBDC som en kontantækvivalent.

Råd

47. Regeringer, der overvejer at implementere en CBDC, bør designe systemer fra bunden med økonomisk inklusion i tankerne. Dette betyder meningsfulde handicaptilpasninger fra starten og nøje overvejelse af alle befolkningsgruppers særlige omstændigheder. Visse designvalg vil sandsynligvis øge udbredelsen af CBDC'er og også øge inklusionen. Disse omfatter offline- og peer-to-peer-betalingsmuligheder, uigenkaldelig fortrolighed for transaktioner i detailhandelsstørrelse, transparent og interoperabelt design og tilgængelige digitale tegnebøger, der beskytter privatlivets fred.

48. Regeringer bør også adressere inklusion fra starten i deres politikker. Specifik opsøgende indsats over for marginaliserede befolkningsgrupper kan fremskynde implementeringen, og regeringer bør være omhyggelige med at tilbyde tilgængelige støttetjenester for at integrere enkeltpersoner i systemet og fejlfinde problemer.

49. Bedre kontrol med hvidvaskning af penge kunne fokusere på reduceret fortrolighed for transaktioner over en vis tærskelværdi og andre målrettede interventioner. CBDC-systemer bør udformes til at begrænse regeringers beføjelse til fuldt ud at udelukke enkeltpersoner fra adgang til en digital valuta. Tekniske og organisatoriske foranstaltninger kan overvejes for at dele beføjelsen til kritiske handlinger mellem flere enheder. Som et eksempel kunne en kryptografisk nøgle, der er nødvendig for at udføre en kritisk operation, opdeles og distribueres mellem flere enheder ("hemmelig deling"). Denne foranstaltning kunne være nyttig mere generelt til at implementere fælles forvaltning af kritiske handlinger, der har en stærk indvirkning på enkeltpersoners rettigheder og frihed.

5.5 Samlet vedtagelse og anvendelse af en CBDC: nødvendighed og proportionalitet

50. Ved beskyttelse af privatlivets fred og grundlæggende rettigheder er det to væsentlige kriterier at fastslå nødvendigheden af at behandle visse personoplysninger og at foretage en operationel proportionalitet, der afvejer indgreb i den personlige sfære i forhold til de forfulgte mål.

51. Med disse to kriterier i tankerne er etableringen af en CBDC en kritisk beslutning, der skal overveje både fordele og omkostninger, idet der ikke kun tages hensyn til økonomiske aspekter, men også eventuelle skadelige konsekvenser for samfundet og individets rettigheder, herunder beskyttelse af privatlivets fred og personoplysninger.

[37] I USA har nogle medlemmer af Kongressen og Senatet for eksempel vurderet, at politikker mod hvidvaskning af penge i uforholdsmæssig høj grad har ramt arabiske og muslimske amerikanere og immigranter, hvilket har resulteret i, at amerikanere uden forbindelse til terrorisme eller økonomisk kriminalitet nægtes adgang til banktjenester. Se brev fra Elizabeth Warren, Ilhan Omar et al. til amerikanske bankmyndigheder om modernisering af sanktions- og anti-hvidvasknings-/financial crimes-overholdelsespolitikker, den amerikanske kongres (2. december 2022), https://files.constantcontact.com/d51f5406801/55723f25-4c19-4c8c-ad57-943dbd461b2f.pdf.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

52. Hvis nødvendighed og proportionalitet ikke nøje overvejes i hele processen med at oprette en CBDC, kan CBDC-systemet øve unødvendig og uforholdsmæssig stor indblanding i grundlæggende rettigheder, herunder beskyttelse af privatlivets fred og personoplysninger, i strid med, hvad der forventes i et demokratisk samfund. CBDC's politiske mål, identificerede roller og ansvarsområder, funktioner, der skal implementeres, planlagte arkitektur- og designvalg og den mulige anvendelse af nye teknologier, der medfører specifikke risici, skal alle evalueres ud fra et nødvendigheds- og proportionalitetsperspektiv.

Råd

53. Implementeringen af CBDC-projekter bør være drevet af et klart og dokumenteret behov for en digital valuta. Det betyder, at beslutningstagere og centralbanker nøje bør overveje, om en CBDC er nødvendig for at nå deres mål, såsom at forbedre den finansielle inklusion, reducere transaktionsomkostninger eller forbedre transmissionen af pengepolitikken. Implementeringen af en CBDC bør ikke udelukkende være drevet af ønsket om at holde trit med teknologiske tendenser eller konkurrere med andre digitale valutaer. Medmindre der er et klart og dokumenteret behov for CBDC'en, vil risiciene for privatlivets fred og databeskyttelse sandsynligvis opveje fordelene ved at oprette en CBDC. Ved at sikre, at implementeringen af CBDC'en er drevet af et klart og dokumenteret behov, kan beslutningstagere og centralbanker bedre afveje risiciene for privatlivets fred og databeskyttelse forbundet med CBDC'er mod disse behov, når de beslutter, om de skal gå videre.38

54. Når disse behov er identificeret, bør designet af CBDC baseres på en tilgang, der fokuserer på privatlivs- og databeskyttelse gennem design og som standardfunktioner39. Der bør i planlægningsfaserne udføres en konsekvensanalyse af privatlivs- og databeskyttelse, der tager hensyn til de bredere konsekvenser for grundlæggende rettigheder, for at evaluere virkningen af de planlagte funktioner og anvendelsesscenarier på enkeltpersoners rettigheder og friheder. Der bør også udføres regelmæssige vurderinger under implementeringen, da nogle risici og konsekvenser muligvis ikke er synlige, før teknologien er i brug.

55. De identificerede risici og virkninger bør føre til identifikation af passende afbødende foranstaltninger. Et CBDC-projekt bør udformes på en måde, der minimerer indsamling og brug af personoplysninger ved at sikre, at kun de nødvendige oplysninger indsamles og behandles. Desuden bør de mindst indgribende processer og teknologier identificeres og implementeres. Hvis niveauet af indgriben, på trods af indsatsen i denne retning, stadig ikke er acceptabelt ud fra et proportionalitetssynspunkt, skal udviklerne genoverveje det planlagte design, funktionaliteter, informationsbehandling

[38] For et eksempel på vurdering (ingen godkendelse): Bank of England. Central Bank Digital Currency: muligheder, udfordringer design. (2020). https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper . Tilgængelig på

[39] Se for eksempel EDPB's retningslinjer 4/2019 om artikel 25 i databeskyttelse gennem design og som standard. Trods De er baseret på Den Europæiske Unions GDPR og indeholder nyttige anbefalinger og forslag til alle interessenter. Findes på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en .

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

arkitektur og protokoller, der er nødvendige for at reducere virkningen, helt op til at opgive projektet, om nødvendigt.[40] Samarbejde mellem beslutningstagere, centralbanker, finansielle tjenesteydelsesregulatorer og databeskyttelsesmyndigheder er et vigtigt element i at forstå og forudse skader på privatlivets fred. Derudover er engagement mellem beslutningstagere, centralbanker, finansielle tjenesteydelsesregulatorer og databeskyttelsesmyndigheder en effektiv måde at opnå den offentlige tillid, der er nødvendig for en udbredt anvendelse. Disse myndigheder bør benytte sig af (eller udvikle) muligheder for dialog og samarbejde, såsom aftalememoranda, digitale regulatoriske samarbejdsfora, regulatoriske sandkasser og ad hoc-høringsforanstaltninger[41] .

6. Privatlivsrisici ved visse specifikke valg eller komponenter

56. I dette afsnit fremhæver vi et kort udvalg af nogle privatlivsrisici og relevante råd om specifikke valg for CBDC-design eller -komponenter. Nedenstående overvejelser er ikke udtømmende, men et eksempel, der kan være nyttigt for beslutningstagere og (hvis relevant) centralbanker, når de vedtager rammer og tekniske funktioner for CBDC'er.

6.1. Brugen af distribueret ledgerteknologi (DLT)

Beskrivelse

57. En distribueret ledger er "en database, der deles og synkroniseres på tværs af netværk, spredt på tværs af flere steder, institutioner eller geografiske områder, hvilket giver transaktioner mulighed for at have [flere private eller] offentlige 'vidner'".[42] Blockchain er et eksempel på en DLT.

58. DLT-baserede systemer bruger en distribueret hovedbog til at registrere og verificere transaktioner. Hver deltager på netværket har en kopi af hovedbogen, og eventuelle ændringer i hovedbogen skal verificeres af en konsensusmekanisme, før de endeligt tilføjes. Deltagerne er normalt en række forskellige aktører, såsom banker, betalingstjenesteudbydere og andre finansielle institutioner.[43]

[40] Grimm, R., & Böhme, R. (2021). "Digitale centralbankvalutaer: Et privatlivsperspektiv." I Proceedings of the 17. internationale konference om privatliv, sikkerhed og tillid (PST).

[41] Databeskyttelsesmyndighederne kan tilbyde ekspertise om risici og foranstaltninger til at afbøde dem og håndtere dem. databeskyttelseskrav, såsom principperne om nødvendighed, proportionalitet og dataminimering; datastyrings- og risikovurderingsprocessen, herunder konsekvensanalyser af databeskyttelse; problemer med datadelingsaftaler; og eventuelle andre krav i henhold til gældende databeskyttelseslovgivning.

[42] VERDENSØKONOMISK FORUM, INNOVATIONSDREVEN CYBERRISIKO FOR KUNDEDATA I FINANSIELLE TJENESTER – HVIDBOG 6 (2017), https://www.weforum.org/whitepapers/innovation-driven-cyber-risk-to-customer-data-infinancial-service .

[43] Hvad angår Riksbankens e-Krona-projekt, se https://www.riksbank.se/en-gb/payments-- for yderligere information. kontanter/e-krone/teknisk-løsning-til-e-krona-pilotprojektet/.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Machine Translated by Google

59. Når en transaktion er tilføjet til hovedbogen, er den uigenkaldelig, hvilket giver en høj grad af uforanderlighed og sikkerhed. Brugen af kryptografi sikrer, at kun autoriserede parter kan få adgang til hovedbogen, og at transaktioner autentificeres og krypteres for at sikre fortrolighed.44

60. Selvom mange DLT-baserede applikationer ikke begrænser brugernes deltagelse i systemet, er et DLT-baseret CBDC-system normalt konfigureret til kun at tillade autoriserede noder at deltage i netværket. Her fører centralbanken tilsyn med systemstyringen og afviklingsoperationerne og sikrer, at det fungerer effektivt, sikkert og i overensstemmelse med lovgivningsmæssige og juridiske krav. Derudover administrerer den netværksnoderne, opdaterer softwaren og sikrer systemets skalerbarhed og robusthed.45

61. Historisk set har centralbanker eksperimenteret i vid udstrækning med DLT'er, til dels påvirket af private aktørers indsats for at udstede og forvalte private digitale penge såsom Bitcoin. De angiveligt identificerede fordele med hensyn til integritet og gennemsigtighed samt potentiel brug af smarte kontrakter til programmerbare penge påvirker også brugen af DLT. Dens distribuerede nodeinfrastruktur og konsensusbaserede drift indebærer, at DLT-arkitektur ofte overvejes til operationer såsom engrosbetalinger mellem centralbanker og relevante formidlere46 samt grænseoverskridende betalinger.47

62. CBDC-projekter verden over, der bruger DLT-baserede afviklingssystemer, omfatter:

- Kinas digitale valuta elektroniske betaling (DCEP). Den digitale yuan, der er udviklet af People's Bank of China, er en digital version af Kinas fiatvaluta, renminbi.48
- Sveriges e-krone. Riksbanken, Sveriges centralbank, undersøger udviklingen af e-Krona, en foreslået CBDC, der ville bruge DLT-baseret teknologi.49

44 Swan, M. (2015). "Blockchain: en plan for en ny økonomi." O'Reilly Media, Inc – tilgængelig på https://www.oreilly.com/library/view/blockchain/9781491920480/.

45 BIS-arbejdspapirer – nr. 1015, DLT-baseret forbedring af effektiviteten af grænseoverskridende betalinger – en juridisk og Regulatorisk perspektiv, maj 2002. Tilgængelig på: https://www.bis.org/publ/work1015.pdf.

46 Afmystificering af digital valuta for centralbanker i engrosleddet, tale af Fabio Panetta, medlem af den udøvende magt ECB's bestyrelse, på symposiet om "Betalinger og værdipapirafvikling i Europa - i dag og i morgen", 26. september 2002.

47 Verdensbankgruppen, Centralbankens digitale valutaer til grænseoverskridende betalinger, En gennemgang af aktuelle eksperimenter og idéer, november 2021, tilgængelig på: https://documents1.worldbank.org/curated/en/369001638871862939/pdf/Central-Bank-Digital-Currencies-for-Cross-border-Payments-A-Review-of-Current-Experiments-and-Ideas.pdf .

48 For yderligere information, se People's Bank of China. "Digital valuta (DC/EP)." https://www.pbc.gov.cn/en/3688110/index.html.

49 For yderligere information, se Riksbanken. "E-Krona-projektet." https://www.riksbank.se/en-gb/payments--kontanter/e-krone/.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

• Digital euro: Til backend-prototypen udviklede Eurosystemet en centraliseret afviklingsmotor (N€XT) baseret på output af ubrugte transaktioner (UTXO).50

Risici

63. At stole på en DLT-arkitektur indebærer ikke nødvendigvis en mere privatlivsvenlig løsning. Manglende fortrolighed er en risiko at overveje, når man implementerer et DLT-baseret afviklingssystem. Faktisk er data, der er lagret i distribuerede ledgere, native synlige for alle deltagere på netværket. Dette skaber en høj grad af gennemsigtighed og revisionsbarhed, hvilket kan være nyttigt til at forhindre svindel og hvidvaskning af penge. Det giver dog også anledning til bekymring om privatliv og fortrolighed, da personlige oplysninger såsom transaktionsbeløb og kontosaldi kan være synlige for andre parter på netværket, hvis der ikke er tilstrækkelige kontroller på plads, på en måde, der forringer privatlivsbeskyttelsen, selv med hensyn til det nuværende betalingsskema. Denne mangel på fortrolighed kan afskrække nogle brugere fra at bruge CBDC'er.51

64. Uforanderligheden af DLT-løsninger, såsom blockchain, skal også tages i betragtning. I en DLT kan data, når de først er blevet skrevet til ledgeren, ikke ændres eller slettes. Selvom uforanderlighed giver betydelige fordele med hensyn til integritet, udgør den også potentielle privatlivsrisici. Især når personoplysninger skrives til blockchainen, kan de ikke fjernes eller korrigeres. Dette skaber betydelige udfordringer for overholdelsen af databeskyttelsesrettigheder, såsom retten til berigtigelse, "retten til sletning" eller "retten til at blive glemt".

Råd

65. Begræns personoplysninger på kæden: Data, der skrives direkte til kæden, bør begrænses, muligvis kun til ikke-personoplysninger. Andre personoplysninger kan være 'off-chain', og kun de oplysninger, der er strengt nødvendige for at forbinde til og redegøre for betaleren og modtageren, vil blive gemt på kæden.

66. Giv brugerne mere kontrol over deres personlige oplysninger, såsom muligheden for selektivt at videregive bestemte transaktionsoplysninger til bestemte parter (det være sig centralbanker eller formidlere), eller muligheden for at bruge pseudonymer til at maskere deres identiteter. Dette kan bidrage til at afbalancere behovet for gennemsigtighed med behovet for privatliv og fortrolighed.52

---

[50] For yderligere information, se Den Europæiske Centralbank (2023), Digital euro – Prototypeoversigt og erfaringer.
lært, tilgængelig på
https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf.

[51] Cocco, L., Pinna, A., & Marchesi, M. (2017). "Banking på blockchain: omkostningsbesparelser takket være blockchain-teknologi." Journal of Financial Perspectives, 5(3), 18-31.

[52] Den Europæiske Centralbank, I FOKUS - Nummer 4, december 2019, Udforskning af anonymitet i centralbankers digitale systemer valutaer. Tilgængelig på: https://
www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

67. Design det DLT-baserede system til at inkludere privatlivsfremmende funktioner, såsom nul-vidensbeviser, som kan bidrage til at bevare fortroligheden af transaktionsoplysninger, samtidig med at integriteten og sikkerheden af ledgeren opretholdes.53

68. Verificér, om det er muligt at opnå tilsvarende (eller bedre) funktioner og ydeevner ved at bruge ikke-DLT-teknologi.54 For eksempel kunne smarte kontrakter eller PET'er designes uden nødvendigvis at bruge DLT.55

6.2. CBDC-programmerbarhed

69. CBDC-programmerbarhed betyder, at visse finansielle begivenheder kan programmeres til at finde sted, når de udløses af andre begivenheder. Generelt skelnes der i litteraturen mellem programmerbarhed af betalinger og programmerbarhed af penge.56

Beskrivelse

Programmerbare betalinger

70. Programmerbare betalinger er betalinger, der udføres automatisk, når visse betingelser er opfyldt, baseret på forudbestemte regler. Dette er ikke en ny funktion, som CBDC'er kan introducere, da programmerbare betalinger allerede findes i nuværende bankbetalingssystemer (f.eks. stående ordrer eller direkte debiteringer). I nuværende CBDC-planer er programmerbare betalinger relateret til brugen af smarte kontrakter57 baseret på DLT-teknologi.

71. Programmerbare betalinger i en CBDC muliggør udførelse af tidsbundne transaktioner. Denne funktion kan være nyttig i scenarier som lønsystemer, hvor lønninger kan udbetales automatisk på forudbestemte datoer. Den letter også automatiseringen af tilbagevendende betalinger, abonnementer og kontraktlige forpligtelser. I et forsyningskædescenarie kan betaling for varer udløses automatisk, når leveringsbekræftelsen er modtaget. Denne funktion sikrer sikre og gennemsigtige betalinger, samtidig med at risikoen for svindel eller manglende overholdelse af kontraktvilkår reduceres. Endelig kan programmerbare betalinger i en CBDC muliggøre flerparts escrow-aftaler, så midler

53 Gross, Jonas og Sedlmeir, Johannes og Seiter, Simon, Sådan designer du en kompatibel, privatlivsbevarende fiat stablecoin med nul viden (december 2022). på SSRN: https://ssrn.com/abstract=4331465 eller http://dx.doi.org/10.2139/ssrn.4331465 Via Beviser 15, Tilgængelig

54 Se fodnote 46.

55 Olaf Owe, Elahe Fazeldehkordi, En letvægtsmetode til smarte kontrakter, der understøtter sikkerhed, tryghed og privatliv, Journal of Logical and Algebraic Methods in Programming, bind 127, 2022, 100772. Tilgængelig på: https://doi.org/10.1016/j.jlamp.2022.100772 .

56 A. Bechtel, J. Gross, P. Sandner, V. von Wachter, Programmerbare penge og programmerbare betalinger, 29. september 2020. Tilgængelig på: https://jonasgross.medium.com/programmable-money-and-programmable-payments-c0f06bbcd569 .

57 Singh, Jaskaran, Programmerbare betalinger og smarte kontrakter (15. juli 2022). Tilgængelig på SSRN: https://ssrn.com/abstract=4215442 eller http://dx.doi.org/10.2139/ssrn.4215442

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

overføres ikke, før alle involverede parter opfylder deres forpligtelser. Denne anvendelse kan være gavnlig for komplekse transaktioner, såsom køb af fast ejendom eller crowdfunding-kampagner, hvor frigivelsen af midler er betinget af opfyldelse af foruddefinerede betingelser fra flere parter. Programmerbare betalinger øger tillid og sikkerhed ved at automatisere escrow-processen, reducere behovet for mellemmænd og minimere risikoen for tvister.

Eksempler på CBDC-projekter rundt om i verden, der overvejer brugen af programmerbare betalinger, er: Digital Baht-projektet fra Bank of Thailand58, Sydkoreas digitale won59 og Den Europæiske Centralbanks digitale euro60

Programmerbare penge

72. Programmerbar penge refererer til evnen til at inkorporere foruddefinerede regler og betingelser i selve den digitale valuta. Det betyder, at CBDC'en kan designes med evnen til automatisk at udføre transaktioner baseret på foruddefinerede kriterier. Igen er smarte kontrakter det mest udforskede eksempel på denne type teknologi.

73. Et eksempel på programmerbare penges muligheder ville være, når en regering beslutter at fordele et specifikt beløb til bestemte borgere til kulturelle formål, med den betingelse, at disse midler ikke kan anvendes til andre formål. Regeringen kan indkode reglerne og betingelserne i selve CBDC'en og dermed sikre, at midlerne udelukkende afsættes til kulturelle aktiviteter. Betalingen kan automatisk blokeres, hvis den ikke er rettet mod de tilsigtede formål. På denne måde giver programmerbare penge et stærkt værktøj for regeringer, centralbanker og andre myndigheder til at udøve kontrol over brugen af midler og sikre, at de anvendes til specifikke formål eller inden for foruddefinerede parametre.

74. Programmerbar valuta kan muliggøre realtidsovervågning og revision af specifikke transaktioner, hvilket forbedrer det lovgivningsmæssige tilsyn. Ved at integrere programmerbare funktioner i en CBDC kan myndighederne spore pengestrømmen, identificere mistænkelige mønstre eller aktiviteter og håndhæve krav til transaktionsrapportering.

75. Derudover kan programmerbare penge bruges til at automatisere overholdelse af lovgivningsmæssige rammer. Ved at inkorporere de relevante regler og betingelser i CBDC-infrastrukturen kan behovet for manuel indgriben og overholdelseskontroller reduceres. På denne måde kan CBDC'en automatisk håndhæve lovgivningsmæssige krav, såsom at begrænse størrelsen af transaktioner, implementere handelsrestriktioner eller sikre overholdelse af skatteforpligtelser.

---

[58] Se https://www.bot.or.th/en/financial-innovation/digital-finance/central-bank-digital-currency.html https://www.bok.or.kr/eng/main/contents.do?menuNo=400411 Se ECB-dokument:

[59]

[60] https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221110_item32programmerbarebetalinger.en.pdf

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

76. Eksempler på CBDC-projekter rundt om i verden, der anvender programmerbare penge, omfatter:

- Kinas digitale valuta elektroniske betaling (DCEP). Den digitale yuan er designet til at tillade programmerbare funktioner såsom begrænsninger på brug, udløbsdatoer og smarte kontraktfunktioner.61

- Sveriges e-krone.62 E-krona-projektet fra Sveriges Riksbank, Sveriges centralbank, overvejer programmerbare pengefunktioner. E-kronen sigter mod at muliggøre programmerbare funktioner såsom tidsbegrænsede betalinger og transaktionsbetingelser gennem smarte kontrakter.

Risici

77. Programmerbarhedsfunktioner i CBDC involverer i sagens natur automatiserede beslutningstagningsbestemmelser, hvor algoritmer og smarte kontrakter udfører transaktioner og håndhæver foruddefinerede regler. Disse automatiserede processer analyserer data og anvender foruddefinerede algoritmer til at træffe beslutninger i realtid, såsom at verificere transaktioners gyldighed, håndhæve kontraktvilkår eller bestemme berettigelse til specifikke finansielle tjenester. Det er dog afgørende at sikre, at sådanne automatiserede beslutningsprocesser overholder juridiske og etiske standarder, især i forhold til databeskyttelsesprincipper og individuelle rettigheder, såsom gennemsigtighed og retten til at gøre indsigelse, indhente menneskelig gennemgang og anfægte automatiserede beslutninger.

78. Forskellige programmerbare funktioner i en CBDC indebærer forskellige risici for privatlivets fred og borgerrettigheder, der kan opveje de potentielle fordele. For eksempel skaber begrænsninger på, hvor penge kan bruges, betydelige risici for censur og marginalisering af aktiviteter eller endda befolkningsgrupper, som regeringer anser for uønskede. Tidsbegrænsninger for at bruge en valuta kan derimod skabe mange af de samme politiske fordele, såsom at forhindre valutahamstring og yde økonomisk stimulus uden at involvere regeringen i at beslutte, hvilke virksomheder der er "værdige".

Råd

79. Gennemsigtighed og ansvarlighed er væsentlige krav i en CBDC, og især programmerbare pengesystemer. Organisationer skal give enkeltpersoner klare oplysninger om, hvordan deres data behandles, logikken bag automatiseret beslutningstagning og de sikkerhedsforanstaltninger, der er indført for at sikre retfærdighed og nøjagtighed. Privatlivspolitikker bør beskrive databehandlingspraksis og enkeltpersoners rettigheder, så brugerne kan udøve deres rettigheder, når de deltager i programmerbare pengesystemer.

80. Når automatiseret beslutningstagning påvirker enkeltpersoner væsentligt, skal der sikres en meningsfuld menneskelig indgriben, der giver enkeltpersoner mulighed for at anfægte beslutninger truffet udelukkende af algoritmer, og retten til at indhente meningsfuld information om den logik, der er involveret i beslutningen.

---

[61] Se fodnote 48
[62] Se fodnote 46

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Machine Translated by Google

automatiseret beslutningsproces og effektiv afhjælpning, når det er nødvendigt. Organisationer, der driver programmerbare pengesystemer, skal implementere mekanismer, der muliggør dette.

81. Lovgivere bør overveje, om visse programmerbare pengefunktioner, der potentielt kan have en alvorlig indvirkning på individers friheder og demokrati (f.eks. forhindre individer eller en kategori af individer i at bruge penge i en bestemt sammenhæng), nogensinde bør planlægges for at undgå, at disse kan blive ulovligt udnyttet.

7. Argumenter for peer-to-peer online og offline betalinger

82. Peer-to-peer onlinebetalinger er typiske betalingsordninger for kryptovalutaer, hvor penge kan overføres direkte uden behov for mellemmænd, såsom en centralbank, kommercielle banker eller betalingsudbydere, hvilket kan strømline betalingsprocessen og reducere finansielle omkostninger samt fremme økonomisk inklusion af personer uden bankforbindelse. Peer-to-peer onlinebetalinger kan også være komponenter i en CBDC i tilfælde, hvor det er blevet fastslået, at der ikke er behov for formidling eller øjeblikkelig afvikling af den enkelte transaktion. Peer-to-peer-betalinger, herunder i forbindelse med en CBDC-ordning, kan også finde sted mellem to offline-enheder (tokens), der lagrer valuta.

83. Peer-to-peer-betalinger spores ikke af centralbanker og formidlere, hvilket sikrer indbygget privatliv. Da transaktioner finder sted direkte mellem parter, har brugerne mere kontrol over deres personlige oplysninger og kan nyde bedre privatliv sammenlignet med traditionelle, formidlede og kontobaserede betalingssystemer. CBDC-transaktionernes peer-to-peer-karakter eliminerer eller reducerer afhængigheden af centraliserede formidlere, hvorved deres indsamling og lagring af personoplysninger udelukkes eller minimeres. Dette kan bidrage til at afbøde bekymringer vedrørende potentiel misbrug af personoplysninger af formidlere eller risikoen for databrud.

84. Peer-to-peer-betalinger er normalt kun blevet overvejet under visse omstændigheder, da deres struktur kan hindre ansvarlighed og revisionsbarhed, samt nødvendige AML/CFT-kontroller. Normalt er de, hvis nogen, tilladt for transaktioner under et bestemt beløb eller under hensyntagen til en transaktionsbeløbsgrænse inden for en bestemt tidsramme.

85. Beslutningen om at implementere en peer-to-peer-funktion i en CBDC afhænger af forskellige faktorer, herunder det ønskede niveau af finansiel formidling, behovet for regulatorisk tilsyn og de overordnede mål om finansiel inklusion (for personer uden bankkontor) og effektivitet. Derfor bestemmes tilstedeværelsen eller fraværet af en peer-to-peer-komponent i en CBDC i sidste ende af centralbankens og de styrende myndigheders specifikke politiske mål.

86. Derudover indebærer online peer-to-peer-betalinger stadig visse databeskyttelsesrisici. Generelt kan de, selvom de er tilladt under begrænsede omstændigheder, dele den samme grundlæggende infrastruktur og protokoller som formidlede betalinger. Dette indebærer, at der skal anvendes specifikke teknikker for at opretholde den nødvendige fortrolighed i transaktionerne.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

87. Derfor bør CBDC-systemet kun indsamle og opbevare nødvendige metadata, samtidig med at videregivelsen af personligt identificerbare oplysninger minimeres. Der skal overvejes mekanismer, der giver transaktionel validering, samtidig med at brugernes privatliv bevares. Teknikker som nul-vidensbeviser kan undersøges for at muliggøre verifikation uden at afsløre specifikke transaktionsdetaljer og dermed forbedre privatlivets fred i peer-to-peer CBDC-transaktioner.63

88. Offlinebetalinger i forbindelse med en CBDC indebærer deres egne specifikke risici på grund af deres offline-natur og fordi de muliggøres af bærbare enheder såsom smartphones, smartcards og bærbare enheder. Udfordringerne omfatter muligheden for tab eller tyveri af enheder, forfalskning af enheder, det mulige behov for at opdatere deres software, når de normalt er offline, og behovet for at holde den kryptografiske nøgle, der bruges til fortrolighed og sikker autentificering, sikker. Brugen af enheder såsom smartphones, som er multifunktionelle onlineenheder, øger angrebsfladen.

89. Relaterede risici omfatter værditab, svindel (ofte på grund af øjeblikkelig betaling og afvikling) eller dobbeltforbrug (muligheden for at bruge flere gange de værdier, der er gemt i enheden). Det er vigtigt at etablere en specifik risikobaseret tilgang til håndtering af offlinebetalinger64 . Dette er nødvendigt for at skabe en CBDC, der sigter mod at erstatte kontanter og holder løfterne om en privatlivsbevarende løsning,65 både
offline og online.

90. CBDC-projekter rundt om i verden, der overvejer en peer-to-peer-komponent, omfatter:

- Bahamas' Sand Dollar,66 en CBDC designet til øgruppen. Sand Dollar inkluderer en peer-to-peer-komponent, der giver beboere mulighed for at handle direkte med hinanden ved hjælp af den digitale valuta. Denne funktion har til formål at fremme finansiel inklusion og reducere afhængigheden af kontanttransaktioner i fjerntliggende områder, hvilket fremmer økonomisk effektivitet og tilgængelighed.

- Uruguays e-peso.67 Uruguays centralbank er ved at udvikle e-peso, et CBDC-projekt, der inkluderer en peer-to-peer-komponent. E-pesoen sigter mod at forbedre finansiel inklusion, reducere omkostninger og effektivisere betalinger i landet. Med peer-to-peer-funktionaliteten kan enkeltpersoner og virksomheder udføre direkte transaktioner ved hjælp af e-pesoen, hvilket muliggør sikre og problemfri digitale betalinger.

- Sveriges e-krone.68 Sveriges Riksbank, Sveriges centralbank, undersøger udviklingen af en e-krone CBDC. E-krona-projektet inkluderer en peer-to-peer-komponent

63 Se fodnote 21.

64 BIS Projekt Polaris: Del 1: En håndbog til offline betalinger med CBDC, maj 2023. Tilgængelig på: https://www.bis.org/publ/othp64.htm

65 Indledende bemærkning af Fabio Panetta, medlem af ECB's direktion, i Udvalget for Europa-Parlamentets Økonomiske og Monetære Anliggender, 4. september 2023. Tilgængelig på: https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230904~8f5dff1e57.en.html

66 For mere information, se https://www.sanddollar.bs For mere

67 information, se https://www.bis.org/events/eopix_1810/licandro_pres.pdf Se fodnote 46

68

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.

Machine Translated by Google

der giver enkeltpersoner og virksomheder mulighed for at foretage direkte transaktioner ved hjælp af den digitale valuta. Målet er at skabe en sikker og effektiv betalingsinfrastruktur, der kan sameksistere side om side med eksisterende betalingssystemer, hvilket muliggør problemfri peer-to-peer-overførsler.

- Digital euro: Forslaget til forordning om indførelse af en digital euro omfatter en offline-metode til nærhedsbetalinger (P2P).[69]

8. Yderligere læsning

Ud over ovenstående referencer vil vi gerne fremhæve følgende nyttigt læsemateriale.

- EDPB-EDPS fælles udtalelse nr. 02/2023 om forslag til forordning om Den Europæiske Unions Europa-Parlamentets og Rådets forordning om oprettelse af den digitale euro, 18. oktober 2023. Tilgængelig på: https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/2023-10-18-edps-edpb-joint-opinion-digital-euro_en
- Bank of Canadas rapport: "En digital canadisk dollar: Hvad vi hørte 2020-23, og hvad der kommer derefter". Tilgængelig på: https://www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next/
- AEPD blogindlæg om "Digitale valutaer". Findes på: https://www.aepd.es/en/prensa-y-comunicacion/blog/digital-currencies
- Reserve Bank of Australia, "Australian CBDC Pilot for Digital Finance Innovation", projektrapport, august 2023. Tilgængelig på: https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/pdf/australian-cbdc-pilot-for-digital-finance- innovation-project-report.pdf
- BIS Project Aurora, "Kraften ved data, teknologi og samarbejde til at bekæmpe penge" hvidvaskning på tværs af institutioner og grænser", maj 2023. Tilgængelig på: https://www.bis.org/about/bisih/topics/fmis/aurora.htm

[69] Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af det digitale euro COM/2023/369 endelig.

Sekretariat
Forbundskommissær for databeskyttelse og informationsfrihed (BfDI)

Graurheindorfer Str. 153
D-53117 Bonn
Telefon +49 / 228 99/7799 1404

E-mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Arbejdsgruppen støttes af databeskyttelseskommissærer og uafhængige eksperter fra lande over hele verden for at forbedre privatlivets fred og databeskyttelse inden for teknologi.